jc654 U.S. PTO
05/03/99

jc549 U.S. PTO
09/303035
05/03/99

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship ..... Vanzini et al.
Applicant ..... Microsoft Corporation
Attorney's Docket No. MS1-254US
Title: PCMCIA-compliant Smart Card Secured Memory Assembly For Porting User Profiles and Documents

TRANSMITTAL LETTER AND CERTIFICATE OF MAILING

To: Commissioner of Patents and Trademarks
Washington, D.C. 20231

From: Lewis C. Lee (509) 324-9256
Lee & Hayes, PLLC
W. 201 North River Drive, Suite 430
Spokane, WA 99201

The following enumerated items accompany this transmittal letter and are being submitted for the matter identified in the above caption.

1. Transmittal Letter with Certificate of Mailing included.
2. PTO Return Postcard Receipt
3. New patent application (title page plus 27 pages, including claims 1- 38 & Abstract)
4. Executed Declaration
5. 4 sheets of formal drawings (Figs. 1- 5)
6. Assignment w/Recordation Cover Sheet

Large Entity Status [x] Small Entity Status [ ]

The Commissioner is hereby authorized to charge payment of fees or credit overpayments to Deposit Account No. 50-0463 in connection with any patent application filing fees under 37 CFR 1.16, and any processing fees under 37 CFR 1.17.

Date: May 3, 1999

By: _____
Lewis C. Lee
Reg. No. 34,656

CERTIFICATE OF MAILING

I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the below-indicated date. Any Express Mail No. has also been marked on the listed items.

Express Mail No. (if applicable) EL209423130

Date: 5/3/99

By: _____
Dana L. Calhoun

EL209423130

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

09604950 050900

PCMCIA-compliant Smart Card Secured Memory Assembly For Porting User Profiles and Documents

Inventor(s):
Giorgio J. Vanzini
Gregory Burns

ATTORNEY'S DOCKET NO. MS1-254US

TECHNICAL FIELD

This invention relates to systems and methods for transporting user profiles and data files from one computer to another. More particularly, this invention relates to a portable profile carrier that enables a user to securely store and transport a user profile and personal data files, while allowing the user to access the profile and data files during log on processes at a standalone or networked computer so that the computer retains the same 'look and feel' of the user's desktop and setup.

BACKGROUND

Profiles are used by operating systems to configure operating characteristics of a computer (e.g., user interface schema, favorites lists, etc.) according to user-supplied preferences and provide storage for the user's personal data files (e.g., files on the desktop or in the user's "my documents" folder. Windows NT operating systems from Microsoft Corporation supports two types of profiles: local profiles and roaming profiles. A local profile is stored and loaded from a fixed location on the local computer. The profile remains at the computer, and is not portable to another computer. Thus, if the user logs onto another computer, a new profile is created for that user from a default profile. As a result, the user ends up with different profiles on each machine that he/she logs onto and hence, each machine looks and feels differently.

A roaming profile travels with the user in a networked environment and is made available to the user regardless of which machine the user logs onto. Fig. 1 shows a client-server architecture 20 that implements conventional roaming profiles. The architecture 20 includes a server 22 connected to serve a client 24

over a network 26. The server 22 has an operating system 28 and a profile store 30 that holds various user profiles. The profiles are associated with the users via a passcode. The client 24 runs an operating system 32.

When the user logs onto the client 24, the user is initially prompted for a user name, domain name, and password. The domain name is used to identify the server 22 and the user name is used to locate a corresponding user profile from the profile store 30. If a profile exists (i.e. the user name is known to the server), the password is used in a challenge response exchange with the server to verify the identity of the user. If the user provided the correct password for the given user name the user's profile is downloaded from the server 22 to the client 24 and used to configure the client according to the user's preferences.

If additional security is warranted, the architecture may further include smart card tokens. The user is assigned a personal smart card and inserts the smart card into a card reader at the client. In this case the user name, domain name, and password is stored on the smart card. Instead of the user entering this information the user enters a passcode that unlocks the card and makes the information available to the client which then performs the logon process as described above.

One drawback with the roaming architecture is that users have only limited control over their own profiles. A user cannot, for instance, establish a roaming profile without the assistance of a network administrator. The administrator must assign a roaming profile pathname in the user's account on the domain server. The user then has the option to indicate on each machine whether to use a roaming profile or a local profile.

Another drawback with roaming profiles is that the architecture restricts roaming to clients connected to the network 26 with access to the domain server

and the profile server 22. The architecture does not allow a user to access his/her profile on a home computer or other standalone computer that is not network attached.

Accordingly, there is a need for a portable device that securely transports a user's profile and related documents (My Documents) to various machines, regardless of whether the machines are connected or standalone. The inventors have developed such a device.

SUMMARY

This invention concerns a portable profile carrier that stores and securely transports a user's profile and personal user data files from one computer to the next.

The profile carrier is a two-component assembly comprising a storage card (e.g., smart card) and a card reader. The reader is physically constructed in a form factor of a PCMCIA card and has a slot to receive the storage card. The reader has a card interface and controller to facilitate data communication with the storage card.

According to an aspect of this invention, the reader is equipped with data memory (e.g., flash memory) to store the user profile and data files. The storage card protects access to the data memory. The composite profile carrier alternately enables access to the user profile on the flash memory when the card is present and the user is authenticated, while disabling access when the card is removed or the user is not authenticated within a certain time period.

In one implementation, the storage card is implemented as a smart card having processing capabilities. The card reader is implemented as a smart card

reader. The profile assembly is assigned a pair of public and private keys, with the public key being stored on the smart card reader and the private key being kept on the smart card. The smart card also stores a passcode that is unique to the user.

To access the contents in the flash memory, the user assembles the card reader and smart card and inserts the assembled carrier into a PCMCIA device reader at the computer. The user is prompted to enter a passcode and the smart card authenticates the user by comparing the user-supplied passcode to the stored passcode. Assuming that the user is legitimate, the smart card then authenticates the smart card reader by determining whether the public key is complementary with the private key. If it is, access to the user profile and data files on the flash memory is permitted.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a prior art client-server system that supports roaming profiles from one network client to another.

Fig. 2 is a block diagram of system having a portable profile carrier that securely transports user profiles and data files from computer to computer. The portable profile carrier, in conjunction with the computer operating system, enables authenticated access to the profiles and documents at a computer, regardless of whether the computer is standalone or networked.

Fig. 3 is a diagrammatic view of a composite profile carrier that includes a smart card reader and a smart card.

Fig. 4 is a block diagram of the system components, including the computer operating system, smart card, and smart card reader.

Fig. 5 is a flow diagram showing steps in a two-phase authentication process for accessing user profile and data files carried on the profile carrier.

The same numbers are used throughout the figures to reference like components and features.

DETAILED DESCRIPTION

This invention concerns a portable profile carrier for transporting a user profile from one computer to the next in order to configure each computer according to user preferences. The profile carrier is equipped with sufficient memory to hold data files as well as the user profile. In one implementation, the profile and data files are secured, in part, using cryptographic techniques. Accordingly, the following discussion assumes that the reader is familiar with cryptography. For a basic introduction of cryptography, the reader is directed to a text written by Bruce Schneier and entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons with copyright 1994 (second edition 1996).

System

Fig. 2 shows a computer system 50 having a computer 52 and a portable profile carrier 54. The computer 52 has an operating system 56 and a PCMCIA (Personal Computer Memory Card Interface Association) device reader 58 that is capable of reading PCMCIA cards, which are also referred to as PC cards. The computer may be configured as a general-purpose computer (e.g., desktop computer, laptop computer, personal digital assistant, etc.), an ATM (automated teller machine), a kiosk, an automated entry system, a set top box, and the like.

The machine 52 may be a standalone unit or networked to other computers (not shown).

The profile carrier 54 stores a user's profile in a secured medium that can be conveniently transported. The profile consists of user information that can be used to configure computer 52 according to selected preferences and schema of the user. The profile contains essentially all of the information that is useful or personal to the user. For instance, a profile might include a user's name, logon identity, access privileges, user interface preferences (i.e., background, layout, etc.), mouse control preferences (i.e., click speed, etc.), favorites lists, personal address book, the latest electronic mail (sorted according to user criteria) and so forth. One can also envision that application tokens or keys can be stored, and that will allow the user to access or use the applications for which he/she has tokens or keys.

The profile carrier 54 is an assembly of two components: a card reader 60 and a storage card 62. At its most basic form, the storage card 62 has a memory to store a passcode associated with the user. Higher forms of the storage card can be implemented, such as an integrated circuit (IC) card that has both memory and processing capabilities. In particular, the storage card 62 can be implemented as a smart card equipped with private memory for storing private keys (or other user secrets) and processing capabilities, including rudimentary cryptographic functionality (e.g., encryption, decryption, signing, and authentication). Smart card technology enables utilization of private keys without exposing them to the external world.

The card reader 60 provides an interface to read and write data to the storage card 62. The card reader 60 is preferably implemented as a PCMCIA (but

could also be implemented via other means, e.g. via Universal Serial Bus, aka USB) smart card reader that is constructed in a form factor of a PCMCIA card so that it may be compatibly received by the PCMCIA device reader 58 at the computer 52. According to an aspect of this invention, the smart card reader 60 is equipped with data memory, such as flash memory, to hold the user's profile and other data files.

According to this architecture, the two-component profile carrier forms a smart card secured memory assembly that alternately enables access to the user profile on the reader-based flash memory when the smart card is present, while disabling access to the user profile when the smart card is removed. The smart card is associated with the user (e.g., via a passcode, like a ATM card) to ensure that only the legitimate user can access the smart card. In addition, the smart card reader 60 and smart card 62 are associated with one another (e.g., by sharing a public/private key pair) to securely link the legitimate user to the user profile and files stored in the flash memory of the smart card reader 60.

Portable Profile Carrier

Fig. 3 shows the profile assembly 54 in more detail. The smart card reader 60 is sized according to a PCMCIA form factor and includes a PCMCIA compatible connector 64 to accommodate insertion into and communication with the PCMCIA device reader 58 at the computer 52. The smart card reader 60 defines a slot to receive the smart card 62, whereby the smart card 62 can be alternately inserted into the reader slot or removed from the reader slot. When inserted, contacts on the smart card align with an interface 66 in the smart card reader 60 to allow communication between the smart card and reader. The smart

card reader 60 also has a controller 68 coupled between the card interface 66 and connector 64 to facilitates data communication between the computer 52 and the smart card 62.

The smart card reader 60 described thus far is of conventional design. There are existing smart card readers with a PCMCIA form factor. Examples of such smart card readers for PCMCIA are made by SCM Microsystems.

Unlike conventional smart card readers, however, smart card reader 60 is equipped with additional data memory 70 to hold the user profile and user files. The data memory can be implemented as flash memory, on the order of currently up to 128 MB, to hold a substantial amount of user data. The data memory 70 is coupled to the controller 68 via a data bus (not shown) to enable access to the data.

Fig. 4 shows functional components in the computer system 50. Computer 52 includes operating system 56 and reader 58. The operating system 56 has a logon module 80 to facilitate the user logon process. For a Windows NT operating system from Microsoft Corporation, the logon module 80 would be a modified version of the dynamic link library "msgina.dll", a component used by the user logon facility "winlogon.exe".

The operating system 56 also has a smart card and flash memory driver 82. The composite driver 82 is capable of detecting whether the device inserted into the PCMCIA reader 58 is a "combo" device that includes both flash memory and a smart card. The modified logon module ("msgina.dll") is designed to recognize that a profile assembly 54 has been inserted into the PCMCIA reader 58 (or alternatively, has established a USB connection). For discussion purposes, the modified logon module for handling the profile assembly will be referred to as

"picoauth.dll". Logon procedures are described below under the heading "Portable Profile Operation", with reference to Fig. 5.

With continuing reference to Fig. 4, the profile assembly 54 comprises the smart card reader 60 and smart card 62. The smart card reader 60 has connector 64, card interface 66, controller 68, and flash memory 70. A multi-bit bus (not shown) connects the components. The flash memory 70 is partitioned into a public area 84 and a private area 86. A public key 90 is stored in the public area 84 of the flash memory 70 and can be exported from the smart card reader 60. The public key 90 is from a public/private key pair assigned to the profile carrier, with the corresponding private key being kept on the smart card. A user profile 92 and data files 94 are stored in the private area 86 of flash memory 70.

The detailed internal architecture of smart cards varies greatly between smart cards from different manufacturers. For purposes of this discussion, a very simplified view of a typical smart card is used. The smart card 72 has an interface 100, a microcontroller or processor 102, and secured storage 104. The microcontroller 102 is preprogrammed to perform certain cryptographic functions and can read from and write to the secured storage 104. The microcontroller 102 responds to commands sent via the interface 100 and can send data in response to those commands back to the interface.

In this simplified smart card 62, the secured storage 104 contains a passcode 106, a private key 108, and an encryption key 110. Before it will perform any cryptographic functions involving private key 108, the smart card 62 is unlocked by a command sent in via the interface 100 that specifies a passcode matching the stored passcode 106. Once unlocked, the smart card can be instructed by other commands to perform cryptographic functions that involve the

use of the private key 108, without making the private key available outside of the smart card.

The programming of the microcontroller 102 is designed to avoid exposing the passcode 106 and the private key 108. Simply, there are no commands that can be issued to the microcontroller 102 via the interface 100 that will reveal the values of the passcode and the private key. In this manner, the smart card prevents a foreign application from ever inadvertently or intentionally mishandling the passcode and keys in a way that might cause them to be intercepted and compromised. In constructing smart cards, manufacturers take additional measures to ensure that the secured storage is inaccessible even when the smart card is disassembled and electronically probed.

Portable Profile Operation

The system described above enables a user to transport his/her profile and data files on a secured portable device from one computer to the next. The user can upload the user profile from the portable device to the computer and automatically configure the computer to his/her likes and preferences. In this manner, every computer "looks and feels" the same to the user, based on that user's settings and preferences.

The profile carrier is configured as a smart card secured flash memory assembly that alternately enables access to the user profile in flash memory when the smart card is present, while disabling access when the smart card is removed. No connection to a server for remote downloading of profiles is necessary, as the portable profile carrier contains all of the information needed by the computer for customized configuration.

To access the user profile, the user assembles the card reader 60 and smart card 62 by inserting the smart card 62 into the slot in the reader 60 to align the contacts with the card interface 66. The user then inserts the assembled carrier into the PCMCIA device reader 58 at the computer 52. Authorization to access the user profile is achieved through a two-phase authentication process. One phase involves user authentication in which the smart card 62 authenticates the user via a passcode challenge. The second phase concerns assembly authentication in which the smart card 62 authenticates the smart card reader 60 as carrying the profile of the user.

Fig. 5 shows steps in the two-phase authentication process that enables access to the user profile and data files. The steps are performed in a combination of hardware and software resident at the computer 52, smart card reader 60, and smart card 62. The method is also described with additional reference to the system illustrated in Fig. 4.

At step 150, the computer 52 monitors for insertion of a PCMCIA-compatible device in PCMCIA device reader 58. In one implementation, the logon "picoauth.dll" module 80 of operating system 56 continually monitors the PCMCIA device reader 58. When insertion is detected, the picoauth.dll module 80 queries the device to determine whether it is a profile assembly having both flash memory and a smart card. Once the profile assembly is identified, the logon module 80 proceeds with the logon procedure.

At step 152, the computer operating system 56 prompts the user via a dialog box or other type window to enter a passcode, such as a PIN (Personal Identification Number). After the user enters the passcode, the smart card/flash

memory driver 82 sends the user-supplied passcode to the smart card 62 via the computer-based PCMCIA device reader 58 and smart card reader 60 (step 154).

The smart card microcontroller 102 compares the user-supplied passcode to the passcode 106 stored in secured storage 104 (step 156). If the two fail to match (i.e., the "no" branch from step 158), the microcontroller 102 rejects the entered passcode and returns a failure notice (step 160). Conversely, if the two match, the user is said to have been authenticated and the microcontroller 102 will now accept commands that involve cryptographic operations involving the private key 108 and the encryption key 110.

In this manner, the smart card is associated with a particular user through the passcode. Only the legitimate user is assumed to know the passcode and hence, only the legitimate user is able to unlock the smart card.

This passcode challenge completes the user authentication phase of the process. The assembly authentication phase is subsequently initiated to determine whether the flash memory device carries the data of the authenticated user. This phase employs public key cryptography to make this determination. As noted above, the composite profile assembly is assigned a pair of complementary public and private keys, with the public key 90 being stored in flash memory 70 on smart card reader 60 and the corresponding private key 108 being stored in the secured storage 104 of the smart card 62.

At step 164, the smart card/flash memory driver 82 reads the public key 90 from the public area 84 of flash memory 70 on the smart card reader 60. The driver 82 passes the public key 90 to the smart card 62 via the computer-based PCMCIA device reader 58 and smart card reader 60 (step 166). The smart card microcontroller 102 runs a process using the public key 90 and the private key 108

from secured storage 104 to determine whether the keys are complementary (step 168). This step determines whether the smart card reader 60 and smart card 62 are associated with one another and form the user's profile carrier, thereby linking the legitimate user to the user profile and files stored in the flash memory of the profile carrier.

If the public key is not valid (i.e., the "no" branch from step 170), the microcontroller 102 rejects the entered public key and returns a failure notice indicating that the card reader does not correspond to the smart card (step 172). On the other hand, assuming the public key checks out (i.e., the "yes" branch from step 170), the smart card instructs the controller 68 on the smart card reader 60 to enable access to the user profile and data files in the private area 86 of the flash memory 70 (step 174). At this point, the computer is permitted to read the user profile and data files from the flash memory 70 and normal logon processes are continued using the profile data from the flash memory (step 176).

The computer configures the computer according to the user profile. The flash memory is also made available as a peripheral storage device for the computer. The operating system presents an icon or name in a file system user interface to inform the user that the memory is addressable and available.

After the user completes a session at this computer, the user can save any files or other data to the flash memory. The user is then free to remove the profile assembly from the computer and carry it to another computer. The user can then repeat the same operation described above to import his/her profile to the next computer.

The scheme described is secure if the computer 52 can be trusted to correctly pass the public key 90 to the smart card 62, and correctly pass the

accepts/reject response from the smart card 62 to the controller 68. To further protect the private area 86 in the smart card reader 60, the contents of the private area 86 can be encrypted (e.g. DES encryption) using a key that can only be obtained from the smart card 62 after the smart card has been successfully unlocked by the user providing the correct passcode. In this case, the computer 52 must send a command to the smart card 62 via the interface 100 to obtain the encryption key 110, which it passes to the controller 68. The controller uses this key to decrypt the user profile 92 and user documents 94 as the computer makes requests to read this data. Similarly when this data is written back to the reader 60, the controller 68 uses the key to encrypt the data before writing it to the private memory area 86. The smart card will only provide the encryption key if it has been previously unlocked, meaning that a user provided the correct passcode.

Storage Card Implementation

The above processes assume that storage card 62 is an IC card or smart card with processing capabilities in addition to memory. As an alternative implementation, the card 62 may be a storage card without processing capabilities. In this arrangement, the storage card 62 stores the passcode or other access credentials in a memory that is accessible by the card reader 60. During logon, the card reader reads the passcode from the storage card 62 and compares it to the user-supplied passcode. If there is a match, the access to the user profile and data files on the flash memory is permitted.

This alternative implementation is not as secure as the smart card-based implementation. However, it still requires user authentication and possession of

both components of the profile carrier during logon to gain access to the user profile and data files.

Conclusion

Although the invention has been described in language specific to structural features and/or methodological steps, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or steps described. Rather, the specific features and steps are disclosed as preferred forms of implementing the claimed invention.

CLAIMS

1. An assembly comprising:

a device constructed in a form factor of a PCMCIA card, the device having an interface to communicate with a storage card and memory to store user data; and

a removable storage card associated with a user that alternately enables access to the user data on the memory when interfaced with the device interface and disables access to the user data when removed from the device.

2. An assembly as recited in claim 1, wherein the storage card comprises a smart card.

3. An assembly as recited in claim 1, wherein the memory comprises flash memory.

4. An assembly as recited in claim 1, wherein the device stores a user's profile that can be used to configure a computer.

5. An assembly as recited in claim 1, wherein the storage card stores a passcode and access to the user data in the memory of the device is enabled upon authentication of a user-supplied passcode to the passcode stored on the storage card.

6. An assembly as recited in claim 1, wherein the device stores a public key and the storage card stores a corresponding private key and access to the user data in the memory of the device is enabled upon verification that the public key and the private key are associated.

7. A profile carrier comprising:

a storage card to store a passcode associated with a user;

a PCMCIA device constructed in a form factor of a PCMCIA card, the PCMCIA device having an interface to communicate with the storage card and a memory to store a profile of the user; and

wherein the assembly permits access to the user profile in the memory of the PCMCIA device upon authentication of the user at the storage card via passcode verification.

8. A profile carrier as recited in claim 7, wherein the storage card comprises a smart card.

9. A profile carrier as recited in claim 7, wherein the memory comprises flash memory.

10. A profile carrier as recited in claim 7, wherein the PCMCIA device also stores data files.

11. A profile carrier as recited in claim 7, wherein the PCMCIA device stores a public key and the storage card stores a corresponding private key, and the assembly permits access to the user profile in the memory of the PCMCIA device upon verification that the public key and the private key are associated.

12. An assembly comprising:

a smart card to store a passcode and a private key from a private/public key pair;

a PCMCIA device constructed in a form factor of a PCMCIA card, the PCMCIA device having an interface to communicate with the smart card and flash memory to store user data and a public key from the private/public key pair;

the smart card being configured to permit use of the private key following validation of a user-entered passcode with the stored passcode;

the smart card being further configured to authenticate the public key stored on the memory of the PCMCIA device using the private key; and

the PCMCIA device being configured to permit access to the user data stored on the memory upon successful authentication of the public key at the smart card.

13. An assembly as recited in claim 12, wherein the PCMCIA device also stores a user profile for use in configuring a computer.

14. A device comprising:

a card reader constructed in a form factor of a PCMCIA card, the card reader being configured to read information from a storage card;

data memory resident in the card reader to store user data; and

a controller resident in the card reader to enable access to the user data in the data memory in response to the card reader receiving access enabling information from a storage card.

15. A device as recited in claim 14, wherein the data memory comprises flash memory.

16. A device as recited in claim 14, wherein the data memory stores a user profile for use in configuring a computer.

17. An assembly, comprising:

the device as recited in claim 14; and

a storage card that can be alternately interfaced with the card reader and removed from the card reader.

18. A computer system, comprising:

a computer having a PCMCIA device reader; and

the assembly as recited in claim 17, wherein the assembly is interfaced with the computer via the PCMCIA device reader so that the computer can access the user data on the device.

19. A PCMCIA smart card reader comprising flash memory.

20. An assembly, comprising:

the PCMCIA smart card reader as recited in claim 19; and

a smart card that can be alternately interfaced with the smart card reader and removed from the smart card reader.

21. A computer system, comprising:

a computer having a PCMCIA device reader; and

the assembly as recited in claim 20, wherein the assembly is interfaced with the computer via the PCMCIA device reader.

22. A computer system, comprising:

a computer having a PCMCIA device reader; and

a smart card secured memory assembly having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the smart card secured memory assembly having data memory to store user data and a removable smart card that alternately enables access to the user data when present and disables access to the user data when removed.

23. A computer system as recited in claim 22, wherein the data memory comprises flash memory.

24. A computer system as recited in claim 22, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user data.

25. A computer system as recited in claim 22, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

26. A computer system as recited in claim 22, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.

27. A computer system, comprising:

a computer having a PCMCIA device reader;

a portable profile carrier to port a user's profile for configuration of the computer, the profile carrier having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the profile carrier comprising:

(a) a storage card associated with the user;

(b) a storage card reader having an interface to communicate with the storage card and data memory to store the user's profile, the storage

card enabling access to the user data on the data memory of the storage card reader;

wherein when the profile carrier is interfaced with the computer via the PCMCIA device reader, the user's profile is accessible to configure the computer.

28. A computer system as recited in claim 27, wherein the data memory comprises flash memory.

29. A computer system as recited in claim 27, wherein the storage card comprises a smart card.

30. A computer system as recited in claim 29, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile.

31. A computer system as recited in claim 29, wherein:

the smart card stores a first key;

the storage card reader stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key passed in from the storage card reader using the first key as a condition for enabling access to the user's profile.

32. A computer system as recited in claim 29, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the storage card reader stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key passed in from the storage card reader using the private key as a condition for enabling access to the user's profile.

33. A method for porting a user profile for a computer, comprising:

storing a user profile in data memory of a card secured profile carrier, the card secured profile carrier having a reader component with a form factor of a PCMCIA card that is equipped with the data memory and a card component that selectively enables access to the user profile in the data memory when interfaced with the reader component;

interfacing the card component with the reader component to form the card secured profile carrier;

interfacing the card secured profile carrier with the computer; and

reading the user profile from the data memory for use in configuring the computer.

34. A method as recited in claim 33, further comprising interfacing the card secured profile carrier with a different second computer and reading the user profile from the data memory for use in configuring the second computer.

35. A method comprising:

storing user data in a card reader;

storing access credentials on a storage card, the access credentials enabling access to the user data stored on the card reader;

interfacing the storage card with the card reader; and

reading the access credentials from the storage card to enable access to the user data.

36. A method comprising:

storing user data in memory installed in a card reader;

storing a reader-resident key in the memory of the card reader;

storing a card-resident key on an IC (integrated circuit) card, the card-resident key corresponding to the reader-resident key;

storing a passcode on the IC card;

interfacing the IC card with the card reader;

receiving a user-entered passcode;

permitting use of the card-resident key following validation of the user-entered passcode with the passcode stored on the IC card;

passing the reader-resident key from the card reader to the IC card;

authenticating, at the IC card, the reader-resident key using the card-resident key; and

permitting access to the user data stored in the memory of the card reader upon successful authentication of the reader-resident key.

37. In a system having a computer with a PCMCIA device reader and a smart card secured profile carrier having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the smart card secured profile carrier having memory to store a user profile and a removable smart card, computer-readable media resident on the profile carrier having executable instructions comprising:

receiving a user-supplied passcode from the computer;

authenticating the user-supplied passcode with a passcode stored on the profile carrier;

enabling access to a private key on the profile carrier upon successful authentication of the user-supplied passcode;

authenticating a public key associated with the memory using the private key; and

enabling access to the user profile in the memory upon successful authentication of the public key.

38. In a system having a computer with a PCMCIA device reader and a smart card secured profile carrier having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the smart card secured profile carrier having memory to store a user profile and a removable smart card, computer-readable media at the smart card having executable instructions comprising:

receiving a user-supplied passcode from the computer;

authenticating the user-supplied passcode with a passcode stored on the smart card;

enabling access to a private key on the smart card upon successful authentication of the user-supplied passcode;

receiving a public key from the memory;

authenticating the public key using the private key; and

enabling access to the user profile in the memory of the profile carrier upon successful authentication of the public key.

ABSTRACT

A portable profile carrier stores and securely transports a user's profile and data files from one computer to the next. The profile carrier is a two-component assembly comprising a smart card and a PCMCIA smart card reader. The reader is physically constructed in a form factor of a PCMCIA card and has a slot to receive the smart card. The reader has a smart card interface and controller to facilitate data communication with the smart card. The reader is equipped with data memory (e.g., flash memory) to store the user profile and data files. Access to the data memory is protected by the smart card. The composite profile carrier enables access to the user profile on the flash memory when the smart card is present and the user is authenticated, and disables access when the smart card is removed or the user is not authenticated.

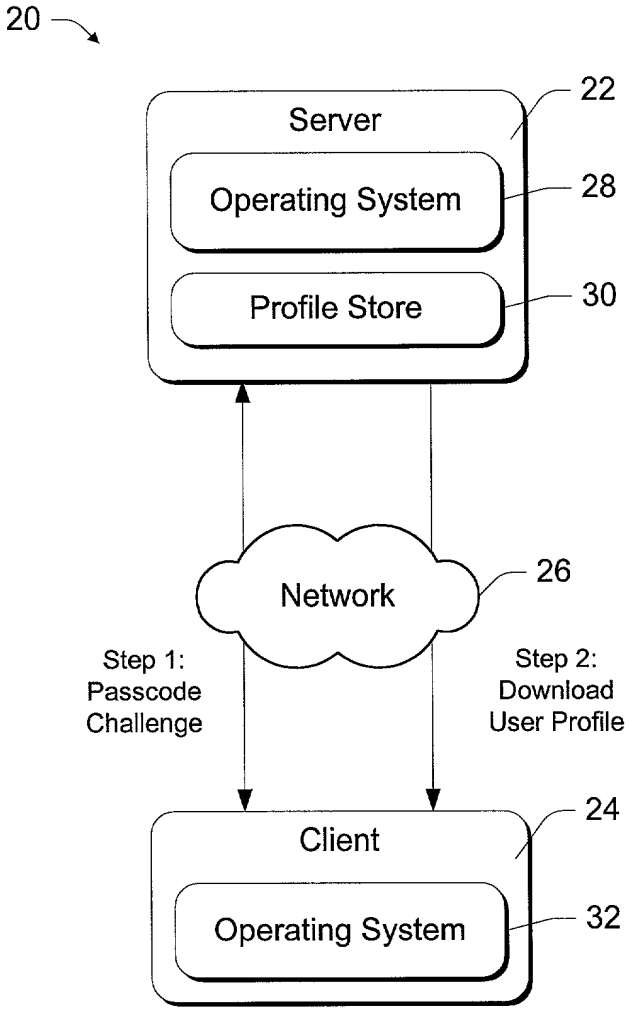

Fig. 1
Prior Art

09504265 - 050909

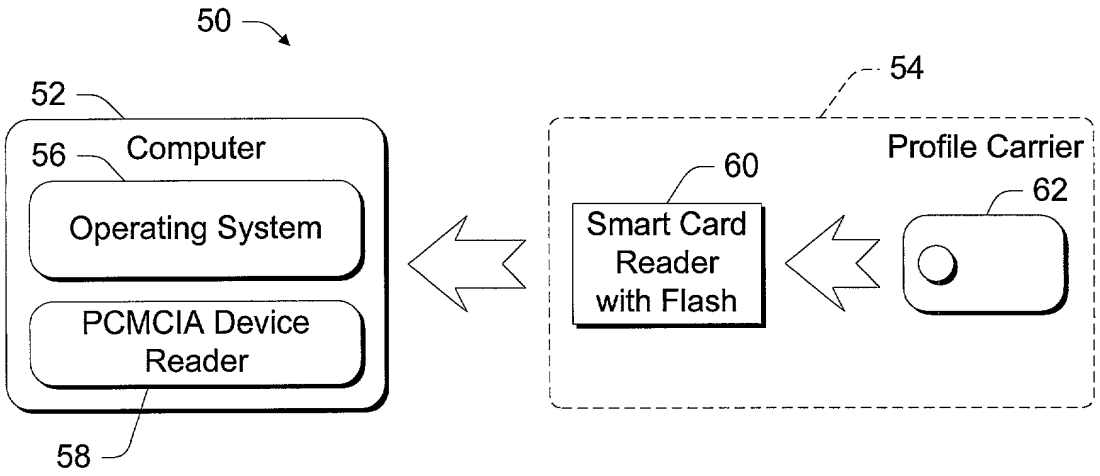

Fig. 2

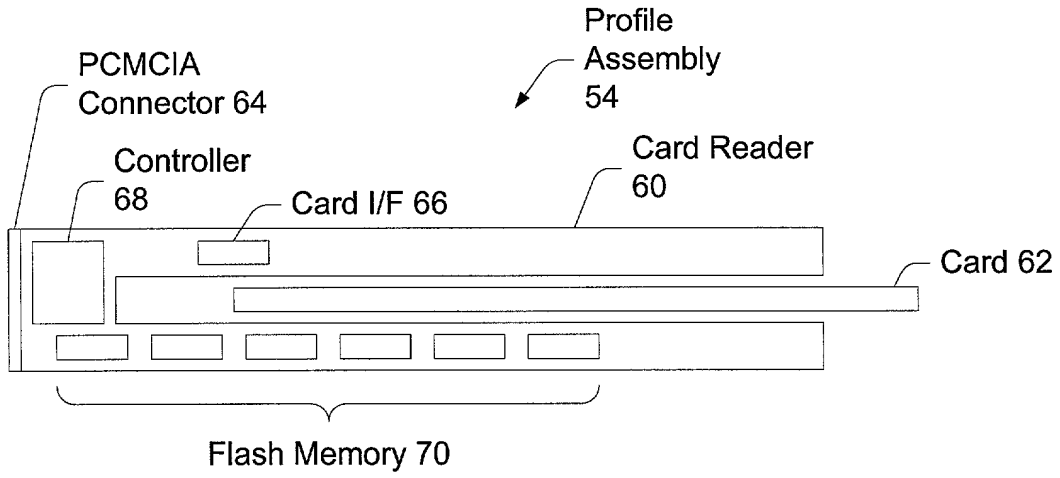

Fig. 3

09905095 - 050905

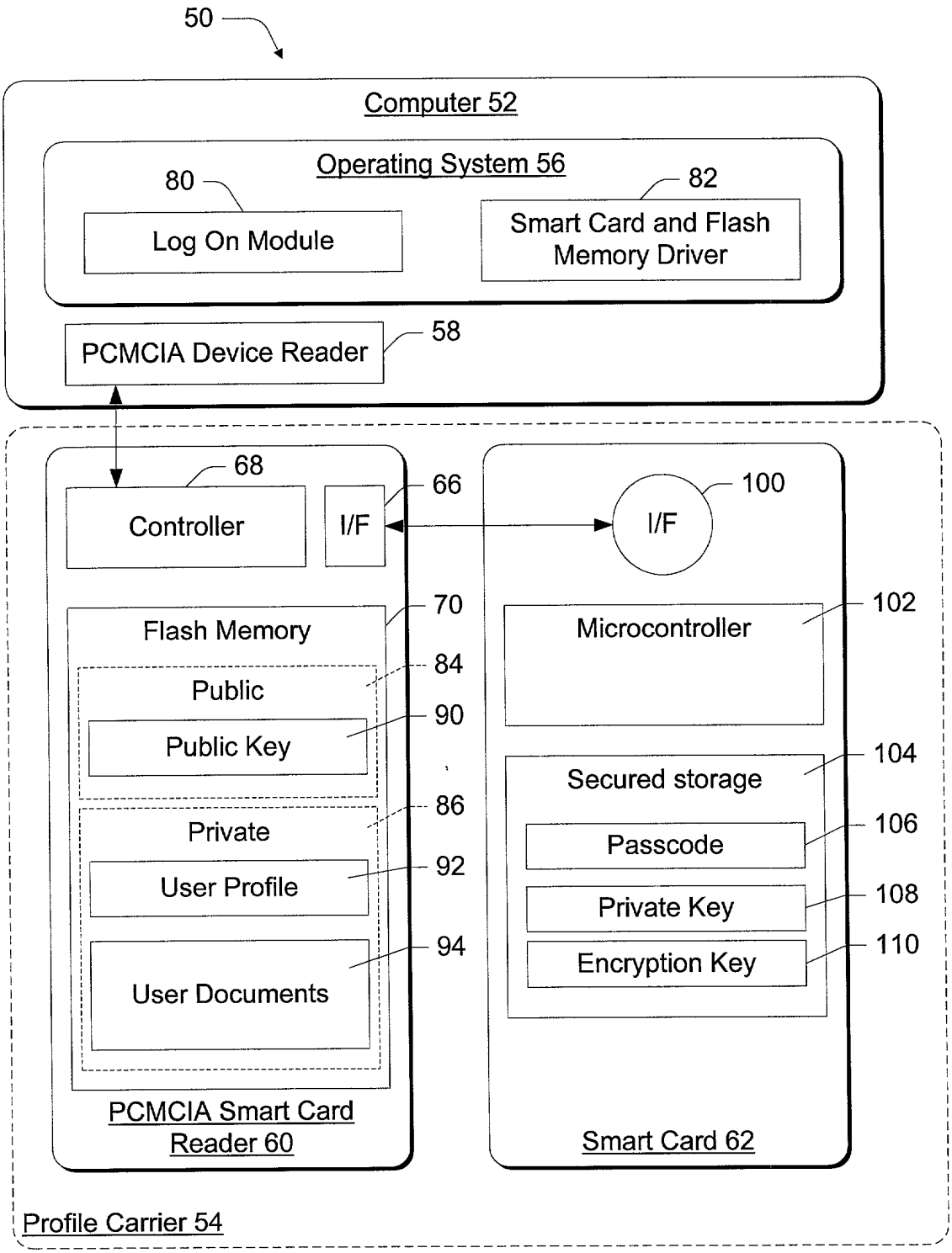
50
Computer 52
Operating System 56
80
Log On Module
82
Smart Card and Flash Memory Driver
PCMCIA Device Reader
58
68
Controller
I/F
66
I/F
100
Flash Memory
70
Public
84
Public Key
90
Private
86
User Profile
92
User Documents
94
Microcontroller
102
Secured storage
104
Passcode
106
Private Key
108
Encryption Key
110
PCMCIA Smart Card Reader 60
Smart Card 62
Profile Carrier 54

Fig. 4

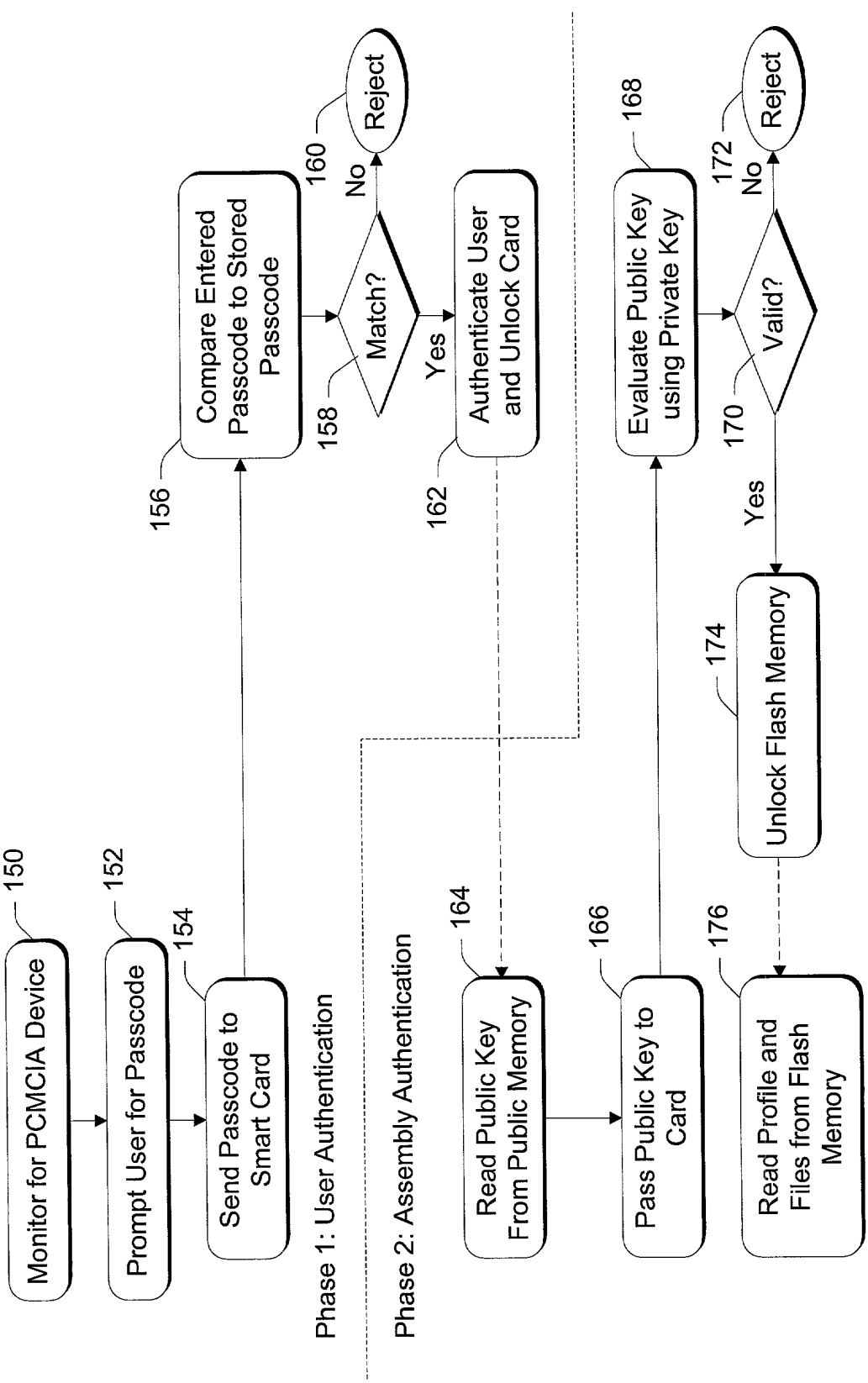
Computer 52
Smart Card Reader 60
Smart Card 62
Monitor for PCMCIA Device
150
Prompt User for Passcode
152
Send Passcode to Smart Card
154
Compare Entered Passcode to Stored Passcode
156
Match?
158
No
160
Reject
Yes
Authenticate User and Unlock Card
162
Phase 1: User Authentication
Phase 2: Assembly Authentication
Read Public Key From Public Memory
164
Pass Public Key to Card
166
Evaluate Public Key using Private Key
168
Valid?
170
No
172
Reject
Yes
Unlock Flash Memory
174
Read Profile and Files from Flash Memory
176

Fig. 5

EL209423130

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship ..... Vanzini et al.
Applicant ..... Microsoft Corporation
Attorney's Docket No. MS1-254US
Title: PCMCIA-compliant Smart Card Secured Memory Assembly For Porting User Profiles and Documents

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "PCMCIA-compliant Smart Card Secured Memory Assembly For Porting User Profiles and Documents," the specification of which is attached hereto.

I have reviewed and understand the content of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATIONS: no applications for foreign patents or inventor's certificates have been filed prior to the date of execution of this declaration.

Power of Attorney

I appoint the following attorneys to prosecute this application and transact all future business in the Patent and Trademark Office connected with this application: Lewis C. Lee, Reg. No. 34,656; Daniel L. Hayes, Reg. No. 34,618; Allan T.

Sponseller, Reg. 38,318, Steven R. Sponseller, Reg. No. 39,384, James R. Banowsky, Reg. No. 37,773, David A. Morasch, Reg. No. 42,905 Katie E. Sako, Reg. No. 32,628 and Daniel D. Crouse, Reg. No. 32,022.

Send correspondence to: LEE & HAYES, PLLC, W. 201 North River Drive, Suite 430, Spokane, Washington, 99201. Direct telephone calls to: Lewis C. Lee (509) 324-9256.

All statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statement may jeopardize the validity of the application or any patent issued therefrom.

* * * * * * * * * *

Full name of inventor:	Giorgio J. Vanzini
Inventor's Signature	G. Vanzini Date: 4/19/99
Residence:	Seattle, WA
Citizenship:	Switzerland
Post Office Address:	741 Boylston Ave E Seattle, WA 98102

* * * * * * * * *

Full name of inventor:	Gregory Burns
Inventor's Signature	Date: 4/19/04
Residence:	Seattle, WA
Citizenship:	British
Post Office Address:	111 West Comstock Street Seattle, WA 98119